Chile: A Vision Of Information Operations

By Igor Carrasco Neira

Mr. Igor Carrasco Neira noted that in his role as a responsible party for critical information protection in Chile, he is most interested in a global reform of the agreement on computer crime. Further, he feels that information will transform social development into a resource, weapon, and target.

Though the image of IO has shown brightly since 1991, especially in light of the First Gulf War, it was not until 1 January 1994—the date when the Zapatista Army of National Liberation (EZLN) uprising was started in Chiapas, Mexico—that we saw the practical effects of an information operation. The EZLN first utilized the Internet as an instrument of war to disseminate its ideas, to raise money, to denounce the Mexican government, and by means of cyberspace recruiting, to attack the networks of the Aztec government by sending massive emailings and computer viruses.

As a contextual fact, until that date the total number of servers connected to the Internet worldwide was 2,217,000. As a result, any given state's use of information technology was low. Yet the Zapatista's IO results could not be qualified in the same way; they gained several advantages from the use of information technology.

What Are the Innovations/ Advantages of the Information Age?

- First, technological advances have actually permitted information-based processes to reach never before seen levels of efficiency;
- Second, there is an increasingly greater dependency on technology systems for handling and transferring information;
- Third, this dependency enabled identification of new vulnerabilities and weaknesses that favor the development of new technologies and procedures for exploiting them, and as a consequence, their countermeasures;
- Fourth, political leaders' interest in rapidly assimilating their respective states into the larger Information Society has grown.

The importance of this assimilation is evident: those who ignore the information age will be left behind, both socially and economically. For example, the multimedia industry, which includes information technology, telecommunications, and mass media, is clearly affected by information age developments. The requirement for economic and societal transformations makes entry conditions into an information society a decisive theme for the future.

Chilean Forces insignia. (Wikipedia)

Today, the cold combination of circuits and metal—the final product of an industrial process—does not make the difference. It is processed information that generates a substantial advantage in social competitiveness. Information now has a leading role in transforming social development into a "resource, weapon, and target." Information has been converted into strategic wealth as well as a condition for competitiveness. Information technologies introduce enormous changes, surpassing pure economics and offering new social, political, and cultural promises through information and communication networks.

The products derived from intellectual activity represent a decisive part of collective wealth. To a large extent, international competitiveness in the new century is a battle of intelligence, that is, of mental models to interpret reality.

The pinnacle of world information networks, such as the Internet, constitutes a considerable challenge for societies. There are evident benefits for the state that uses electronic media, including information media, but also by implication assumption of certain risks—understood to mean the possibility of success or failure—that should be minimized to guarantee information integrity and acceptable service performance. Since 1998, there are well-known reports indicating the presence and execution of programs designed to control and electronically eavesdrop on the different communications of our planet. In February 1999, Director of the US Central Intelligence Agency (CIA) George Tenet, warned that "Various countries have or are developing the capability to attack adversary information systems." He later added, "to develop the capability to attack computers can be inexpensive and ultimately attainable: this requires minimal infrastructure."

National Forces

National information technology security policy came into being in the mid-1990s because of the need to confront the "Y2K" effect. This forced us to prepare for a national catastrophe, or rather, to construct a national map of critical state information infrastructure. Even when primary attention focused on "information errors," the strategic character of information forced the state into an in-depth analysis of the road ahead.

If there is a sector of society experiencing great changes in recent years, it would undoubtedly be in state security and the armed forces. These changes contributed to the promulgation of Law 19.974 in 2004, whose objective is to establish and regulate the State Intelligence System (SIE), which is defined in Article Four (below), and which is chaired by Chile's Director of the National Intelligence Agency (ANI):

Article Four: *The State Intelligence System, henceforth the System, is the collective intelligence organization, ... functionally coordinated, that directs and executes specific intelligence and counter-intelligence activities, to advise the President of the Republic and those various high-levels of leadership of the State, with the objective to protect national sovereignty and to preserve constitutional order and, in addition, formulate intelligence opinions useful for achieving national objectives. The integral organizations of the System, without prejudicing their agencies and their obligations with respect to superior commanders, should interconnect among themselves through the exchange of information and mutual cooperation that this law and the legal code establish.*

The National Intelligence Agency was created in Title Three, Article Seven of the same law:

Article Seven: *The National Intelligence Agency will be created, a centralized public service, of technical and specialized character, which will be subordinate to the President of the Republic through the Interior Ministry, whose objective will be to produce intelligence to advise the President of the Republic and those various high-levels of leadership of the State, in accordance with current law.*

Among the ANI functions under Letter "C" of Article Eight: To propose protective norms and procedures for information systems critical to the State. In this context, national forces are concentrated in two areas: identifying and hardening information networks and infrastructure critical to the State: and creating the capability to influence a potential adversary.

Identification and Hardening of Networks

The tasks conducted in this field range from studies of information flows to reorganizing national networks. To this end, the government sets forth creation of a State Connectivity and Communications Network, through Supreme Decree 5996 of the Interior Ministry.

Presently, the Chilean government is contemplating cybernetic security development within the national technological development plan known as the *Digital Agenda*. The objective of this plan is to increase competitiveness, equal opportunities, individual liberties, quality of life, and the efficiency and transparency of the Chilean public sector through development and employment of information and communication technologies (TIC). At the same time, these actions help enrich the cultural identity of the nation and its native peoples.

The government plan of action for the period 2004-2006 established 34 initiatives, grouped in six areas:

1. Expanded access;
2. Education and training;
3. Online status;
4. Digital development of businesses;
5. Deployment of the TIC industry;
6. Legal framework.

Two of the thirty four initiatives are discussed here: numbers twelve and seventeen. Known as Project 5D, or *The Connective Network of the State*, Initiative Twelve encourages the telecommunications industries to develop a broadband highway voice-and-data-over-IP network for the public sector. It will connect all public branches—including municipalities, schools, hospitals, and clinics—permitting their convergence into a single network of telephone, mobile, and Internet services. Initiative Seventeen establishes a number of Interior Ministry responsibilities: to search and maintain a national response system for cybernetic incidents; administer programs; reduce threats and vulnerabilities; develop security training programs; secure the cyberspace in which the government works; and administer national and international cooperation in cybernetic security matters.

Other decrees to improve cyber security include new technical norms to provide for the confidentiality of electronic documents. These measures establish steps for the public ministries and services to meet security standard ISO 17779, and specify security responsibilities for information circulating on state institutional networks.

Creating the Capability to Influence Potential Adversaries

Naturally, the most serious efforts to create capabilities to influence adversaries utilize information technology resources for training armed forces personnel. This is particularly critical given that modern conflicts are very different from only a few decades ago. In fact, the advance of technology is in direct relation to the decrease of men on the battlefield. Historical examples confirm that during the US Civil War, the "density of men" was approximately 8,200 soldiers per square kilometer. According to NATO doctrine, during the years 1985-1990 there were approximately 400 men per square kilometer. After observing the current war in Iraq, we estimate a density of 15-17 soldiers per square kilometer.

This decrease is due to better armament which is increasingly more lethal, more precise, and lighter weight, but also due to better prepared soldiers. We find that soldiers have greater access to information technology, beginning early in their schooling. This enables the capability to direct things, people, and equipment with greater efficiency. It also allows for the introduction of computer system training directly into the military environment.

Presently, there is an organization within the Chilean War Academy dedicated to this type of training: the Computerized Tactical Operation Training Center (CEOTAC). The center's fundamental objective is to prepare officers, but includes developing the software necessary for this task: the SETAC (Tactical Training System). This advanced military simulator

Chile in its South American context. (CIA)

replicates modern combat conditions in the computer, thus reducing associated training costs. This same center created the Institution and Organization Management Training System (SEGIO) software that prepares civil organizations for emergency situations.

The technology has been very useful in educating soldiers, as well as in instructing them in weapons-handling and marksmanship techniques. The Bernardo O'Higgins Military School has a virtual firing range, with two screens that can project fixed or moving targets, offering the cadets a sensation of reality. The range includes all principal Chilean Army weapons: the Famae 5.56mm rifle, the Beretta 9mm pistol, and the Minimi 5.56mm submachine gun—all of which can be loaded, and produce a shot recoil effect. All of the preceding training saves resources, and results in excellent marksmen. Such technologies enable realistic training, produce a higher quality Chilean soldier, and produce a deterrent effect on potential adversaries.

Combating Crime and Terrorism: Legal Status in Chile

In 1993, Chile ratified Law Number 19.223, which typified legal precepts relating to information technology. Following the French model, this law marked a milestone in Chilean legislation, since it introduced penalties for a number of IT-associated behaviors. The intention was to protect the quality, purity, and suitability of associated information.

The law was important for penalizing unlawful access to computer systems, altering and damaging computer data, and divulging such data. Nevertheless, continuous TIC innovations require consideration of a global reform on computer crimes agreements. Two bills seeking to reform our criminal code on this matter. Both initiatives address a similar type of criminal technical processing: the predominance of the protected legal right as a systematized factor. The first is a parliamentary motion that tackles reform of Law 19.223 on information technology crimes:

- Unlawfully accessing information contained in a computer system;
- Destroying a computer system or altering its function;
- Unlawfully obtaining telecommunication services.

The second corresponds to an executive message categorizing new methods that are not criminalized in our legislation, such as computer crimes:

- Falsification of electronic documents and credit cards;
- Computer fraud;
- Unlawfully obtaining telecommunication services.

Both of these initiatives are currently being processed in the Chilean National Congress. In short, the aforementioned actions seek to solve legal problems that have arisen through introduction of new types of criminal offences, or modification of existing offences based on traditional legal rights.

Chilean International Actions

In order to address the numerous international challenges related to this matter, the Special Policy Director (DIPESP) of the Foreign Affairs Ministry established an Inter-Institutional Working Group on Cybernetic Crime in 2004. The group is made up of representatives from the Interior Ministry, the National Intelligence Agency, the Justice Ministry, the Attorney General, and the Investigative Police. Among their objectives are strengthening cooperative links with other countries, as well as promoting and deepening an information exchange to confront emerging threats in this area.

Thus far, Chile has conducted international actions primarily at the regional level: The Inter-American Commission against Terrorism (CICTE); the Meeting of American Justice Ministries (REMJA) under the OAS; the General Assembly of the OAS; plus the fields of APEC and the United Nations.

In the framework of the REMJA, Chile actively participated in the Third Meeting of the Group of Government Experts on Matters Relating to Cybernetic Crimes, in 2003. A series of recommendations arose from this meeting that are still relevant, and we believe the international community should provide appropriate follow-up on these issues.

Agreement of the European Council on Cybercrime: The Chilean Position

In order to define our country's position regarding eventually joining the Agreement of the European Council on Cybercrime, Chile requested reports from all institutions competent in this matter. In general terms, members favored an eventual Chilean entry into this part of the agreement.

Besides scrutinizing the methodologies and results of the 2004 Fifth Meeting of the American Justice Ministries or Attorney Generals, Chilean representatives noted recommendations for State members to "evaluate the benefit of applying the principles of the Agreement of the European Council on Cybernetic Crimes (2001) and consider the possibility of joining this agreement."

Intelligence and Globalization

Themes addressing intelligence are more complicated, given the scenarios that arise from globalization. Although this process presents advantages and opportunities for society, it also gives rise to new conflicts. Emerging areas of struggle range from the research, the knowledge, the industry, and the resulting commerce, to new forms of crime that lend support to criminal organizations, insurgents, or global terrorists.

Information Technology Attack as a Threat

Knowing about and protecting against computer attacks on Chile's infrastructure is indispensable for functioning information and communication systems. Further, such knowledge is critical for public administration of the country's vital businesses—energy, electricity, telecommunications, fuel supply, transportation services, health services, and security among others. The majority of these services administer their productive processes remotely through computer networks, and in real time, thus these have become mandatory tasks.

This subject demands a relevant example. In this context, it is certainly necessary to protect information networks, but also to clearly determine the origin and motivation of the perpetrators, given that the state's response will be completely different if the attacker is a criminal hacker, or a hostile action by another nation-state.

Other data also provides evidence of the magnitude of technological dependency and the requirement for its protection. In 1983, there were a total of 562 computers connected to the Internet across the entire world. In 1993, the number rose to 1,200,000 computers. By June 2005, counting only broadband connections, in Chile alone there were 594,000 computers connected to the Internet. Today the number exceeds one million broadband connections. Thus in two years, there has been more than a 60% increase in Chile alone.

Conclusions

All future scenarios must consider the state's dependence on information systems and complex computing technologies, where many control processes are made in real time and from a distance. As a result, these will be extremely sensitive—if they are not already—and will be likely targets of hostile action from Internet and network experts.

Looking to the future, we see the high probability of increasing dependence on these applied technologies:

- Cheap solar energy;
- Rural Wireless communications;
- Genetically modified food;
- Rapid biotesting through nanotechnology;
- Filters and catalysts for purifying and decontaminating water;
- Managed application of medicines;
- Hybrid vehicles;
- Wireless computers;
- Quantum cryptography.

Finally, to end with the words of authors John Arquilla and David Ronfeldt, "The information revolution alters the nature of conflict and introduces new modalities in the art of war, terrorism, and crime." Chile is in the process of preparing to meet these threats, and more.